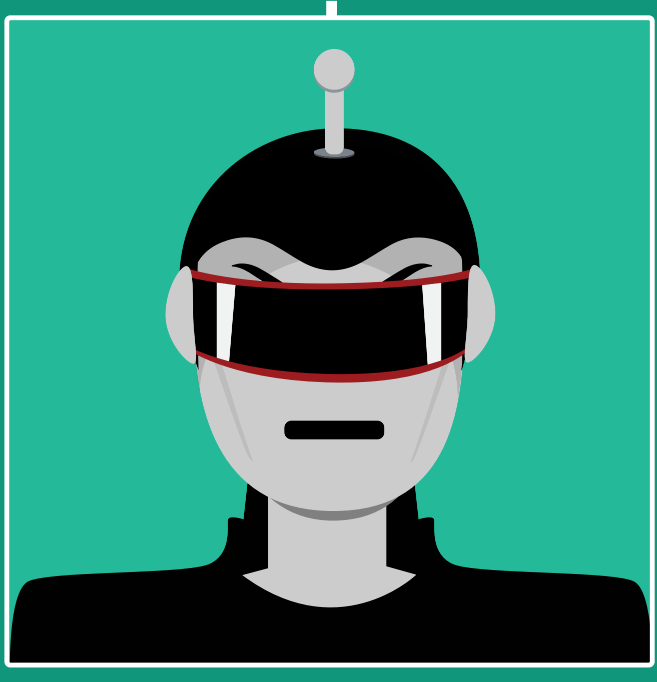
WHO IS ATTACKING YOUR WORDPRESS WEBSITE



SINGLE BOT

An automated computer that can attack one site at a time or a small number of sites simultaneously. Usually unsophisticated attacks.

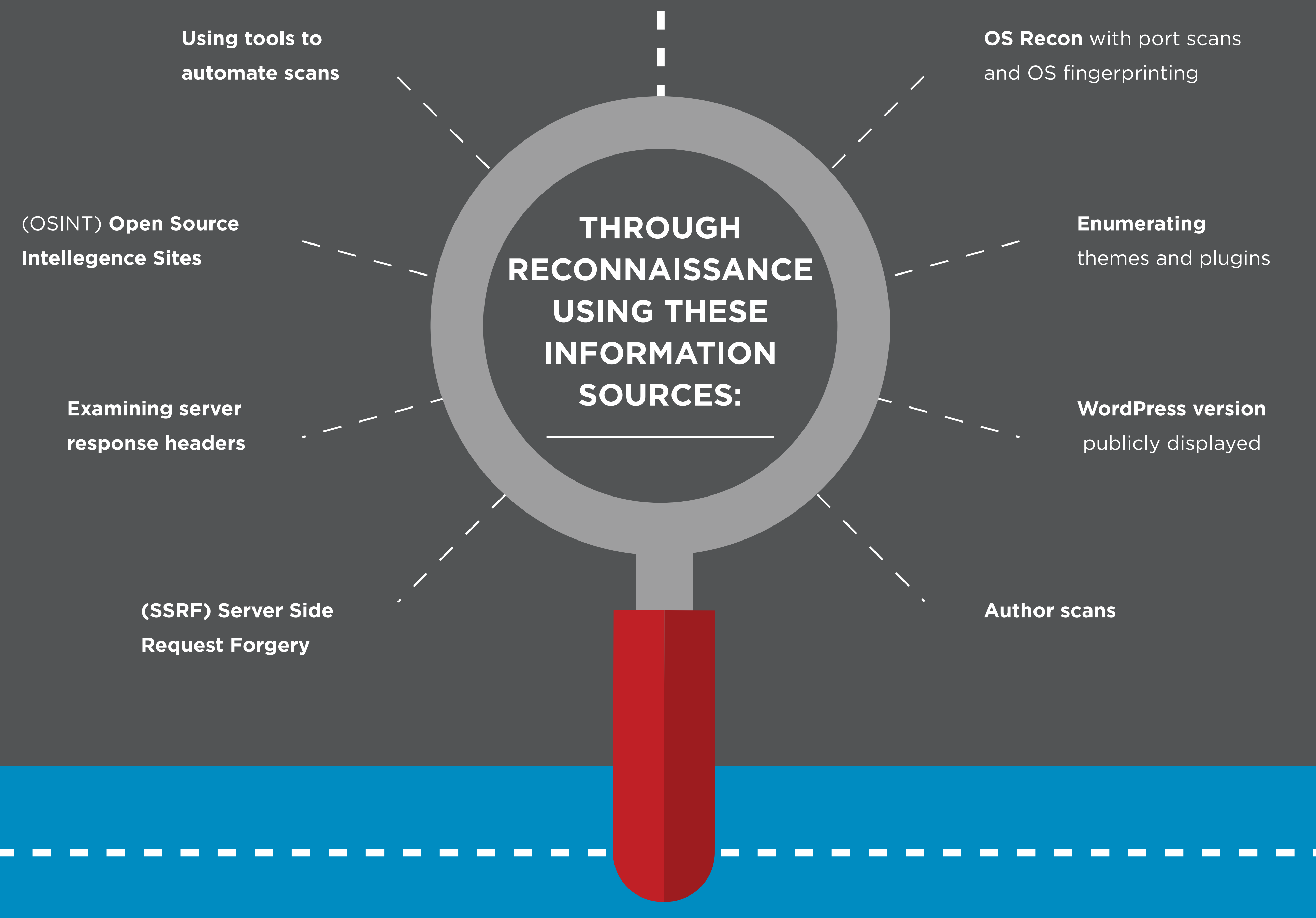
PERSON

Operates a computer manually, attacks one site at a time, slow in attacking but thorough.

BOTNET

A group of computers, can be thousands, attacking multiple sites simultaneously and rapidly. Attacks are unsophisticated but can originate from multiple IP's which add complexity.

How do they get information?



THROUGH RECONNAISSANCE USING THESE INFORMATION SOURCES:

- **Using tools to automate scans**
- **OS Recon** with port scans and OS fingerprinting
- (OSINT) **Open Source Intellegence Sites**
- **Enumerating** themes and plugins
- **Examining server response headers**
- **WordPress version** publicly displayed
- **(SSRF) Server Side Request Forgery**
- **Author scans**

What is being attacked on WordPress sites?

VULNERABILITIES IN PHP CODE INCLUDING WORDPRESS CORE, THEMES, PLUGINS AND OTHER PHP APPLICATIONS:

RCE – Remote Code Execution
SQLi – SQL Injection
XSS – Cross Site Scripting attacks

CSRF – Cross Site Request Forgery
PHP Object Injection
RFI – Remote file inclusion

Authentication Bypass
XXE – External Entity Expansion
(an XML based attack)

PRIVILEGE ESCALATION

- A ordinary user with non-admin access can find a way to escalate their privileges to 'admin' level access

THE LOGIN PAGE VIA:

- Brute force attacks
- Recon to check if usernames exist

OLDER AND UNMAINTAINED WEB APPLICATIONS HOSTED ON THE SAME HOSTING ACCOUNT

- A WordPress install in a subdirectory that is not maintained
- An application like phpmyadmin that is forgotten about and unmaintained
- Backups of your WordPress directory in a subdirectory that are executable PHP and forgotten about

XMLRPC SERVICE

- Brute force logins
- DDoS attacks launched via XMLRPC e.g. Trackback

ON SHARED HOSTING:

- World writable directories. An attacker on the same machine can install a shell on your website.
- Wp-config.php world-readable can give an attacker on the same machine access to your database.
- World-writable files can allow an attacker to execute code as your website.

SOURCE CODE REPOSITORY CONFIG FILES

- .git subdirectory can contain source that is intended to be private
- .svn subdirectory can contain sensitive info

TEMPORARY FILES CREATED BY OTHER APPLICATIONS NOT INTENDED FOR PUBLIC ACCESS

- When the 'vim' editor is used, the temporary file it creates can be web accessible and allow access to sensitive files like wp-config.php containing login credentials for MySQL

ATTACKS THAT TARGET THE OPERATING SYSTEM AND WEB SERVER

- Attacks that target the web server. E.g. Heartbleed
- Attacks that target the operating system services e.g. Shellshock, SSH vulnerabilities, vulnerabilities in other services.

Wordfence™